Technical Notes – Foremost Security Meeting Summary December 17, 2001

Reference: Foremost Security Meeting
Date: Thursday, December 13, 2001
Location: CSMi, Germantown

Outstanding Issues:

Receive database password changing tool(s) from Foremost – they agreed to provide.
What is the maximum length possible for database passwords (i.e. SYSADM)?
Confirm that passwords can contain all printable characters except the semicolon.
Can there be a space (ASCII32) in user names?
What is the maximum length possible for user names?
List which algorithm is used for encrypting passwords when stored in the database.
Will TrueArc enable Foremost in the future to rename database accounts (i.e. SYSADM)?

Comments:

The three-tiered architecture of the Foremost system was explained as outlined on the last page of this document (see diagram, Foremost Architecture).

A. Foremost Enterprise System, Microsoft NT/2K Server
Provides core application layer, interfaces as a broker with both the database and Foremost Document Service. Runs as an NT service. Interfaces with both the database and document server using Foremost system accounts.

B. Database Server, Oracle or MSSQL on any platform
Provides storage for the File Plan, Meta Data, and User Information (includes accounts, security levels, and ACL).

C. Foremost Document Service, Microsoft NT/2K Server
Provides file system storage for the actual records, and runs an NT service that listens to requests via RPC from the broker and responds with records as required.

Although the product is closed-source, the Foremost client API is documented. The documentation is included with the materials provided to DOE. A custom Foremost client can be developed by DOE to meet any additional requirements for the client component that exceed the capabilities of the current software as provided by Foremost (i.e. banner warnings).

Foremost is designed to leverage the capabilities provided by the operating system whenever possible (i.e. rely on Microsoft transports for communication between components, specifically DCOM, ODBC, and RPC).

Recommended implementation synchronizes user accounts with an NT Domain so that Microsoft, not TrueArc, manages user passwords. The product does support its own user account directory, which when synchronized with an NT Domain will not contain any user passwords.

User account credentials are only used for communication between the Foremost Client and the Foremost Enterprise Service. Foremost system account credentials are used for communication between the Foremost Enterprise Service and both the database and Foremost Document Service. At no time does the client communicate directly with the database or Foremost Document Service.

All access control internal to the Foremost application concerning user accounts takes place at the broker-level within the Foremost Enterprise Service.

TrueArc implemented its own access control mechanism that governs which objects in the database and document repository can be accessed by which users, and what permissions those users have in relation to these objects. This system is managed with Access Control Lists and Security Levels. Users can be identified individually, and/or by groups. This access control system is very flexible, and acceptably secure if implemented in an appropriate manner.

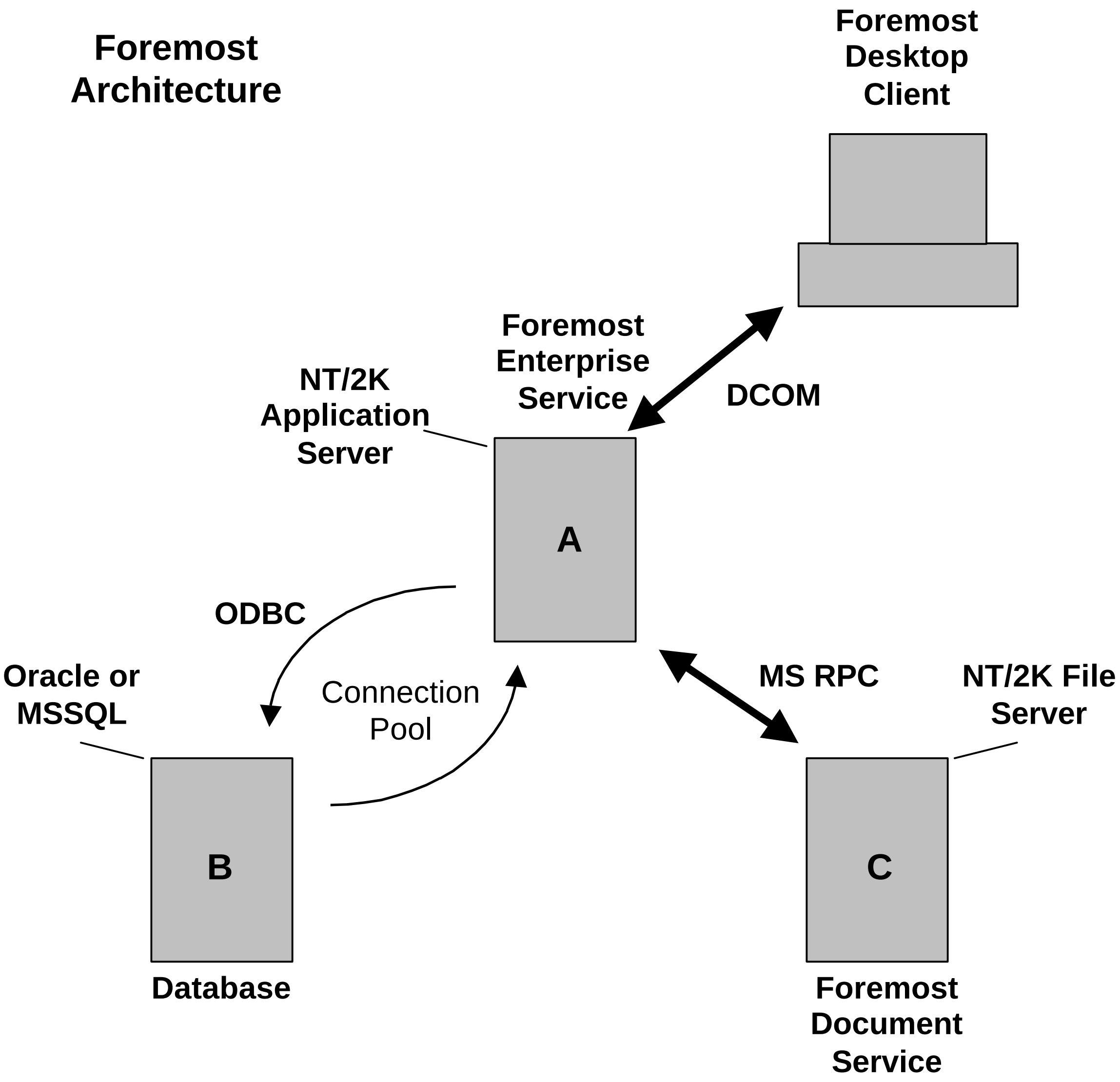
The underlying Microsoft-provided access control lists that govern access to the file system on the file server hosting the Foremost Document Service are not used to limit user access in any way, as users do not communicate directly with this host. The system account defined to run the Foremost service(s) on this host must have full control privileges to the directory tree where files are to be stored.

Service accounts used to run the Foremost Enterprise Service and Foremost Document Service can be any valid Microsoft account with appropriate permissions, and their passwords may be changed using normal methods (i.e. User Manager, and then set correctly in Control Panel, Services).

The Foremost accounts used for communication with the database are currently unable to be renamed, although a procedure to change the passwords for these accounts is documented and a tool to perform this change will be provided by TrueArc.

Application-specific performance logging is not designed into Foremost at this time, but the database can be configured for audit logs. The database can be configured to log events for every access, change, addition, deletion, etc.

TrueArc has not received any security certifications for the Foremost product, although it is certified as meeting the functional guidelines defined in DOD 5015.2.


Foremost Architecture
Foremost Desktop Client
Foremost Enterprise Service
NT/2K Application Server
DCOM
A
ODBC
Connection Pool
Oracle or MSSQL
MS RPC
NT/2K File Server
B
C
Database
Foremost Document Service